UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT BAKER, JR., Defendant.	Case No. 2:10-cr-00119-KJD-GWF **FINDINGS & RECOMMENDATIONS**

This matter is before the Court on Defendant Robert Baker, Jr.'s Motion to Suppress (#43), filed on January 23, 2013; the Government's Response to Motion to Suppress (#44), filed on January 28, 2013; and Defendant's Reply to Government's Response (#46), filed on February 4, 2013. The Court conducted a hearing in this matter on March 4, 2013.

FACTUAL BACKGROUND

Defendant Robert Baker, Jr. is charged in a two count indictment with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) and possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). *Indictment (#1)*. The indictment is based on evidence of child pornography allegedly found during the search of the hard drive of Defendant's computer that was seized pursuant to a warrant issued by a Nevada state court judge on July 8, 2008. Defendant argues that the affidavit in support of the search warrant contained false statements or omissions of fact, and that but for the false statements or omissions, probable cause would not have existed to support the issuance of the warrant. Defendant requested that the Court grant an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674 (1978).

. . .

The affidavit in support of the search warrant was prepared by Detective Shannon Tooley of the Las Vegas Metropolitan Police Department (LVMPD). *Motion to Suppress (#43), Exhibit A, Affidavit.* At the time she prepared the affidavit, Detective Tooley was assigned to the Internet Crimes Against Children Task Force (ICACTF). She had been an officer with the LVMPD for 9 years and had been assigned to the ICACTF for seven months. *Affidavit, pg. 1.* Detective Tooley testified at the hearing that she received training on computers and the internet related to the performance of her duties.

Detective Tooley stated in her affidavit that she conducted an undercover session on May 6, 2008 whereby she used eP2P Limewire software, an enhanced version of the publicly available Limewire program, to download child pornography from another peer to peer user. The affidavit further stated that "Limewire is a peer to peer client that accesses the Gnutella Network." The eP2P Limewire software "is specifically set for single source downloads, which means it downloads files from a single user rather than multiple users. Additionally, the software has an embedded mechanism that logs the traffic between the undercover and the subject computer." *Affidavit, pg. 4.* During the undercover session, Detective Tooley used certain keyword searches which are associated with peer to peer files containing images of child pornography. Detective Tooley was able to download fifteen picture files "depicting child pornography from a Gnutella-based user who was assigned the Internet Protocol (IP) address 70.180.171.140." *Id.*[1]

Detective Tooley's affidavit further stated:

> IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the internet or static, meaning the user's IP assigns his computer a unique IP address and the same number is used by the user every time his computer accesses the internet. IP addresses can be equated to home addresses where as no locations may be in possession of the same IP or home address at any time. Within the realm of the internet only one individual may use an Internet IP address at any given time.

---

[1] The affidavit described the images in the fifteen picture files that Detective Tooley downloaded. *Affidavit, pgs. 4-7.* Defendant does not dispute on this motion that the images constitute child pornography within the meaning of 18 U.S.C. §2256(8).

Affidavit, pg. 4.

The affidavit stated that "[a] query of the Maxmind IP Database revealed the IP address 70.180.171.140 resolved to Cox Communications (COX)." *Affidavit, pg. 7.* On May 6, 2008, an administrative subpoena was served on Cox requesting subscriber information for the user assigned IP address 70.180.171.140. Cox responded by providing information showing that on May 6, 2008 IP address 70.180.171.140 was assigned to Robert Baker, 7009 Rotunda Court, Las Vegas, Nevada 89130. Cox also provided the subscriber's social security number and telephone number. *Id.* Information was subpoenaed from Nevada Power which showed that Robert Baker had electrical service at 7009 Rotunda Court. The Clark County Assessor's web page listed Robert Baker as the owner of the property at that address. The affidavit also indicated that an unspecified records check revealed that Robert Baker resided at 7009 Rotunda Court. *Id.*

Detective Tooley also stated in the affidavit that she conducted a drive-by verification of 7009 Rotunda Court on June 16, 2008 during which she observed a Toyota Camry automobile and a Ford Mustang automobile parked in the driveway of the residence. A Ford F350 truck was parked on the street in front of 7009 Rotunda Court. An inquiry to the Nevada Department of Motor Vehicles showed that the Toyota Camry and Ford F350 were registered to Robert Baker, at 7009 Rotunda Court, Las Vegas, Nevada. The Ford Mustang was registered to a Robert C. Nelson, whose address was also listed as 7009 Rotunda Court, Las Vegas, Nevada. *Affidavit, pgs. 7-8.*

Paragraphs 1-25 of the affidavit provided a "Background on Computers, Child Pornography and Exploitation." These paragraphs generally describe the thought processes of individuals who produce, trade, distribute or possess child pornography and the habits and practices of such individuals in using computers and the internet to obtain, distribute and store child pornography.

Paragraph 24 of the affidavit stated as follows:

> A P2P [peer to peer] file transfer is assigned by reference to an Internet Protocol (IP) address. This address, expressed as four groups of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers. Limewire software displays to the user the IP address from which the image is being downloaded. Additionally, third party software, such as CommView, is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file

> came from one or more IP addresses. Such software monitors and logs internet and local network traffic.

Affidavit, pg. 24.

Based on the information set forth in the affidavit, the Nevada state court judge concluded that there was probable cause to search the residence at 7009 Rotunda Court, Las Vegas, Nevada for evidence of the distribution and possession of child pornography.[2] Defendant Baker asserts in his motion that upon entering his house, the police confirmed that there were three other people living in the home. The police, however, focused their search on Robert Baker, searching only rooms under his control and seizing only his computer equipment. *Motion to Suppress (#43), pg. 3*. The Government has not disputed this assertion.

In support of his motion, Defendant submitted the affidavit of his expert witness, Adrian Leon Mare. *Motion (#43), Exhibit C, Mare Affidavit.* Mr. Mare states in his affidavit that Cox Communications, when providing internet service, does not always know the location of a person connecting to the internet. He further states that typically each piece of computer equipment has a unique MAC number. A person connecting to the internet through Cox sends with each information request a particular MAC number, usually the number associated with the connecting modem. Most Cox customers get their modems through Cox. A modem is usually connected to a router. A router can connect to computers and other devices, either inside or outside the location of the router. Multiple users can use the same router at the same time. Wireless networks have a range up to 300 feet and can be extended even further with additional equipment. Generally, multiple residents in a household will likely use the same router. Typically, computers that use the same router will have the same global IP address. Houseguests and visitors in the house wanting to access the internet can use the same router. Some neighborhoods and communities have created networks in which one global IP address is shared between several households. With wireless routers, even someone driving by or parked outside could use the router. Encrypted wireless

[2] The Court was provided with an unsigned copy of the affidavit. It was not provided with a copy of the search warrant.

signals can be accessed using publically available software. It is possible for an amateur to "spoof," or use a fake IP address using publicly available software. Someone using a "spoofed" IP address could duplicate an IP address used by someone in another part of the world. *Mare Affidavit*, ¶¶ 3-18. The Government does not dispute the assertions made in Mr. Mare's affidavit. This Court has considered similar affidavits by Mr. Mare in other cases involving the validity of a warrant to search for child pornography. *See United States v. Carter*, 549 F.Supp.2d 1257, 1262-64 (D.Nev. 2008) and *United States v. Latham*, 2007 WL 4563459, *4-*5 (D.Nev. 2007).

Detective Tooley testified at the hearing before the Court on March 4, 2013. On cross-examination by Defendant's counsel, Detective Tooley acknowledged that the following emphasized statement at page 4 of her affidavit was false:

> IP addresses can be equated to home addresses where as no locations may be in possession of the same IP or home address at any time. **Within the realm of the internet only one individual may use an Internet IP address at any given time.** (Emphasis added)

Detective Tooley also acknowledged that the following emphasized statement in paragraph 24, at page 13 of her declaration was false:

> A P2P [peer to peer] file transfer is assigned by reference to an Internet Protocol (IP) address. **This address, expressed as four groups of numbers separated by decimal points, is unique to a particular computer during an online session.** (Emphasis added)

Detective Tooley testified that the foregoing statements were standard provisions used in LVMPD search warrant affidavits in 2008. She acknowledged that based on her training and experience in May 2008, she knew that that it was possible for more than one computer to use the same IP address at a given time.

DISCUSSION

In *Franks v. Delaware,* 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), the Supreme Court held that the Fourth Amendment entitles a defendant to challenge the validity of a search warrant affidavit if the defendant makes a substantial preliminary showing that (1) the affidavit contains intentionally or recklessly false statements and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause. *See United States v. Martinez–Garcia,* 397 F.3d 1205, 1215 (9th Cir. 2005), *citing United States v. Reeves,* 210 F.3d

1041, 1044 (9th Cir. 2000). *Franks* further states that if the defendant makes a substantial showing that the affidavit contains intentionally or recklessly false statements, "and if, when the material that is the subject of the alleged falsity is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Id.,* at 171–172, 98 S.Ct. 2674. On the other hand, if the remaining content is insufficient to support probable cause, then the defendant is entitled to an evidentiary hearing. *Id.* At such hearing, the defendant has the burden of proof by a preponderance of the evidence to establish that the false statements were deliberately made or were made with a reckless disregard for the truth. *United States v. De Leon,* 955 F.2d 1346, 1348 (9th Cir. 1992).

Under the same standard, the intentional or reckless omission of material facts from the affidavit may render a search warrant invalid under the Fourth Amendment. *United States v. Stanert,* 762 F.2d 775, 778 (9th Cir. 1985); *United States v. Jawara,* 474 F.3d 565, 582 (9th Cir. 2007). In the case of omissions of fact, the court is required to determine whether there would have been probable cause to issue the search warrant if the omitted facts had been included in the affidavit.

In *United States v. Craighead*, 539 F.2d 1073 (9th Cir. 2008), an FBI agent working in an undercover capacity logged onto the Limewire peer-to-peer file sharing network and downloaded files containing images of child pornography that had been placed on the network by a computer with an identified IP address. The IP address was owned by Cox Communications and was assigned to the defendant's residence. Further investigation corroborated that defendant resided at the address listed in the Cox Communication records. The government obtained a search warrant for defendant's residence and images of child pornography were discovered in the defendant's computer. *Id.*, 539 F.3d at 1078-79. The defendant filed a motion to suppress and requested an evidentiary hearing pursuant to *Franks.* In support of his request for a *Franks* hearing, the defendant argued that the FBI agent impermissibly omitted any statements from the affidavit relating to IP spoofing, internet hijacking, and internet theory which would have informed the magistrate judge of the possibility that despite the IP address connection, the files may not have originated on defendant's computer. In rejecting this as grounds for a *Franks* hearing, the court

stated:

> It is true that ''deliberate or reckless omissions of facts that tend to mislead'' can be grounds for a *Franks* hearing. *United States v. Stanert,* 762 F.2d 775, 781 (9th Cir. 1985). However, the omission rule does not require an affiant to provide general information about every possible theory, no matter how unlikely, that would controvert the affiant's good-faith belief that probable cause existed for the search. SA Andrews did not commit a misleading omission by failing to omit [sic] from her affidavit general knowledge about computer hacking that might support how, hypothetically, Craighead may not have downloaded to his own computer the files that SA Andrews downloaded from Craighead's IP address. *See United States v. Kelley,* 482 F.3d 1047, 1053 (9th Cir. 2007) (holding that an affidavit's failure to raise the possibility that emails containing child pornography could have been unsolicited spam was not a misleading omission); *cf. United States v. Hay,* 231 F.3d 630, 638 (9th Cir. 2000) (holding that a district court's failure to consider theories such as spamming or automated bulk downloading that might support the unlikely possibility that the suspect did not actually transmit 19 images of child pornography himself did not constitute error in a probable cause determination).

Craighead, 539 F.3d at 1081.

The circumstances in this case differ somewhat from those in *Craighead* because Detective Tooley's affidavit contained factually incorrect statements that "only one individual may use an Internet IP address at any given time" and that an IP address "is unique to a particular computer during an online session." Detective Tooley acknowledged that she knew at the time the warrant was issued that more than one computer user can access the internet through the same router and modem and can therefore use the same IP address at a given point in time. The affidavit could therefore have misled the issuing judge into believing that there was a more certain link between Defendant Baker's computer and the child pornography images that Detective Tooley downloaded on May 6, 2008.

In this case, an accurately drafted affidavit would have informed the district judge that on May 6, 2008 Detective Tooley downloaded files depicting child pornography from a Gnutella-based user whose computer was assigned the Internet Protocol (IP) address 70.180.171.140. The affidavit would have further informed the district judge that based on information obtained from Cox Communications, that on the date and time Detective Tooley downloaded the images from the computer, IP address 70.180.171.140 corresponded to the CM MAC number, 00:14:6c:96:10:45,

assigned to the computer modem issued to Defendant Baker. *See Motion to Suppress (#43), Exhibit B, pg. 86.* The affidavit would have stated that the 7009 Rotunda Court, Las Vegas, Nevada address listed on the Cox records was confirmed through other sources as Mr. Baker's residential address. The affidavit would have also stated that it was possible for another computer user in the same residence, or within the receiving range of a wireless router connected to Defendant's modem, to connect to the internet through the Defendant's modem using IP address 70.180.171.140. The affidavit would also have informed the judge that it was possible for a person using a different computer and modem to spoof the IP address assigned to Defendant's computer modem on May 6, 2008.

Even as so revised, the affidavit would have still provided sufficient grounds to find probable cause to search Defendant Baker's computer for images of child pornography. *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007) states that the standards for determining probable cause, as spelled out in *Illinois v. Gates*, 462 U.S. 213, 103 S.Ct. 2317 (1983), apply with equal force to cases involving child pornography on a computer. Probable cause means a "fair probability that contraband or evidence is located in a particular place. "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'common sense, practical question.'" *Id.*, citing *United States v. Gourde*, 440 F.3d 1965, 1069 (9th Cir. 2006).

In *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007), the Fifth Circuit held that the possibility that a computer user outside defendant's residence could have used the IP address assigned to defendant's computer to download or transmit child pornography did not defeat probable cause to search the defendant's residence. In rejecting defendant's argument, the court stated:

> But though it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence. *See United States v. Grant,* 218 F.3d 72, 73 (1st Cir. 2000) (stating that ''even discounting for the possibility that an individual other than [defendant] may have been using his account, there was a *fair probability* that [defendant] was the user and that evidence of the user's illegal activities would be found in [defendant's] home'')

> (emphasis in original). ‘‘[P]robable cause does not require proof beyond a reasonable doubt.’’ *Brown,* 941 F.2d at 1302.

Perez, 484 F.3d at 740–41.

In *United States v. Vosburgh*, 602 F.3d 512, 526-27 (3rd Cir. 2010), the court stated that IP addresses are "fairly" unique identifiers that a specific computer has been used on the internet at a particular time. The court noted, however, that there undoubtedly exists the possibility of mischief and mistake with IP addresses. *Id.*, at 527 n. 14. For example, proxy servers can be used to mask IP addresses and "knowledgeable users can 'spoof' the IP addresses of others." *Id.* The court stated that it was confident that defendant's "IP address was a fairly reliable identifier of his computer for probable cause purposes, in light of the total lack of evidence that he was the victim of any mischief." *Id.*

There is no evidence that Detective Tooley or other law enforcement officers received information prior to the issuance of the search warrant (or thereafter) that Defendant's computer had been hacked or that someone outside his residence used his wireless router to access the internet through his computer modem. Nor did the officers have information indicating that anyone had "spoofed" the IP address assigned to Defendant's modem on May 6, 2008. Absent evidence that any of these acts had actually occurred, there was probable cause to believe that the child pornography images that Detective Tooley downloaded on May 6, 2008 were present on Defendant Baker's computer hard drive and would be found during a search thereof. According to the Defendant's motion, upon entering Defendant's residence, the officers immediately focused their search upon Defendant Baker, searching only the rooms under his control and seizing his computer, rather than the computers belonging to other residents. *Motion (#43), pg. 3.* The officers' reported conduct in this regard comported with the probable cause that supported the issuance of the warrant.

CONCLUSION

When Detective Tooley's affidavit is considered without the factual misstatements, and with the inclusion of information that it would have been possible for a computer user other than Defendant Baker to have used IP address 70.180.171.140 on May 6, 2008, the affidavit still

provided sufficient information to support a finding of probable cause to search computers in Defendant Baker's residence at 7009 Rotunda Court, Las Vegas, Nevada 89130 for evidence of child pornography. The Court therefore finds that the search warrant was valid notwithstanding Detective Tooley's acknowledged false statement of facts and the omission of information that arguably should have been included in the affidavit. Accordingly,

RECOMMENDATION

IT IS RECOMMENDED that Defendant's Motion to Suppress (#43) be **denied**.

NOTICE

Pursuant to Local Rule IB 3-2, any objection to this Finding and Recommendation must be in writing and filed with the Clerk of the Court within fourteen (14) days. The Supreme Court has held that the courts of appeal may determine that an appeal has been waived due to the failure to file objections within the specified time. *Thomas v. Arn*, 474 U.S. 140, 142 (1985). This circuit has also held that (1) failure to file objections within the specified time and (2) failure to properly address and brief the objectionable issues waives the right to appeal the District Court's order and/or appeal factual issues from the order of the District Court. *Martinez v. Ylst,* 951 F.2d 1153, 1157 (9th Cir. 1991); *Britt v. Simi Valley United Sch. Dist.*, 708 F.2d 452, 454 (9th Cir. 1983).

DATED this 6th day of March, 2013.

George Foley Jr.

GEORGE FOLEY, JR.
United States Magistrate Judge